Voorstel richtlijn netwerkveiligheid als onderdeel van EU cyber security strategie: naar een open, veilig en betrouwbaar internet?

Toet, J.; Lodder, A.R.

published in
Nederlands tijdschrift voor Europees Recht
2014

DOI (link to publisher)
10.5553/nter/138241202014020002006

document version
Early version, also known as pre-print

Voorstel richtlijn netwerkveiligheid als onderdeel van EU cyber security strategie: naar een open, veilig en betrouwbaar internet?

Trefwoorden: Beveiliging informatiesystemen, cybersecurity strategie, richtlijn

Samenvatting: Het artikel behandelt het voorstel van de Commissie van 7 februari 2013 om een richtlijn in te voeren ter verhoging van het algehele niveau van beveiliging van netwerk- en informatiesystemen in de Europese Unie. Het voorstel vormt een onderdeel van de cybersecurity strategie van de Commissie. De auteurs plaatsen kanttekeningen bij (de effectiviteit van) de gekozen maatregelen en de implementatie daarvan in het licht van een uitgebreide beschrijving van de voorliggende problematiek. Zij onderschrijven evenwel de noodzaak tot het treffen van maatregelen op Europees niveau en sluiten af met hun aanbevelingen ter versterking van het voorstel en de cybersecurity strategie.

Bron: Voorstel voor een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen / COM/2013/048 final*

Joeri Toet & Arno R. Lodder[1]

Inleiding

Op 7 februari 2013 publiceerde de Europese Commissie in de vorm van een integrale cybersecurity strategie haar visie op de aanpak van informatiebeveiligingsproblemen. Als prioriteiten stelt zij onder andere het verhogen van de digitale weerbaarheid, het reduceren van cybercrime en het ontwikkelen van een Europees cyberdefensiebeleid alsmede een internationaal beveiligingsbeleid voor cyberspace. Hiermee streeft de Commissie een veilige en betrouwbare digitale omgeving na en tracht zij de fundamentele Europese rechten en kernwaarden te waarborgen.[2]

Een belangrijk onderdeel van de strategie van de Commissie wordt gevormd door een richtlijn die een hoger gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen beoogt te realiseren (de "**NIB-Richtlijn**").[3] Een voorstel voor deze richtlijn publiceerde de Commissie samen met haar strategie. In dit artikel gaan wij op dit voorstel nader in. Wij behandelen eerst de achtergrond van de problematiek en evalueren vervolgens de maatregelen die de Commissie voorstelt om deze problematiek te adresseren. Wij sluiten af met onze conclusies en enkele aanbevelingen.

Achtergrond van de problematiek

Informatie- en communicatietechnologie ("**ICT**") zijn van cruciaal belang voor het functioneren van onze hedendaagse maatschappij. Aangezien deze afhankelijkheid toeneemt, nemen ook de potentiële negatieve gevolgen van een falen daarvan toe. Het toenemende aantal incidenten leidt ook langzamerhand tot onderkenning van de kwetsbaarheid daarvan en de noodzaak om risico's beter te beheersen.

---

[1] Joeri Toet is advocaat bij De Brauw Blackstone Westbroek N.V. Arno R. Lodder is hoogleraar Internet Governance and Regulation aan de Vrije Universiteit Amsterdam, afdeling Transnational Legal studies.
[2] Europese Commissie, "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*", JOIN(2013)1, 7 februari 2013
[3] Voorstel voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM(2013)48 final - 2013/0027(COD), 7 februari 2013

Informatiebeveiliging en - in bredere zin - het correct functioneren van ICT wordt vaak nagestreefd op basis van het zogenaamde CIA-Model dat staat voor confidentialieit (*confidentiality)*, integriteit (*integrity*) en beschikbaarheid (*availability*). [4] Kwetsbaarheden die kunnen leiden tot tekortkomingen van informatiebeveiliging kunnen verschillende oorzaken hebben. In de eerste plaats kunnen zij het gevolg zijn van gebrekkige hardware of software. Tijdens het ontwikkelproces kunnen daarin (veelal niet direct zichtbare) fouten terechtkomen. Tekortkomingen kunnen ook het gevolg zijn van een onjuist gebruik van technologie. Dat kan gelegen zijn in de implementatie daarvan, zoals wanneer beveiligingsfuncties niet correct worden ingesteld (bijv. toepassing van encryptie op een database). Onjuist gebruik van technologie kan ook gelegen zijn in het eindgebruik, zoals wanneer wachtwoorden worden “uitgeleend”.

Het gevolg van het gebruik van kwetsbare producten en onjuist gebruik is telkens dat informatie en de ICT waarmee die verwerkt wordt, kwetsbaar zijn voor verstoring, uitval en misbruik. Incidenten kunnen zich manifesteren ten gevolge van opzettelijk kwaadwillend handelen. Daarvan is onder andere sprake bij cybercrime, hacktivisme of spionage. Dit soort aanvallen blijken in aantal en complexiteit toe te nemen en zijn bovendien vaak in het nieuws.[5] Wellicht ligt er daarom zoveel nadruk op. Men realisere zich dat de meeste incidenten evenwel het gevolg zijn van fouten in systemen en bij het gebruik daarvan.[6] Uitval kan ook het gevolg zijn van overmacht, zoals branden en natuurrampen. Illustratief is de brand die in 2012 een telefooncentrale van Vodafone platlegde.[7] Het is belangrijk om in te zien dat het bestrijden van kwaadwillend handelen ander ingrijpen vereist dan het voorkomen van fouten bij het ontwikkelen en gebruiken van ICT producten.

Begrip van de oorzaak van beveiligingsproblemen is noodzakelijk voor het bepalen van de gewenste aanpak daarvan. Onprofessioneel handelen door fabrikanten en gebruikers vraagt om een andere aanpak dan misbruik van ICT. Waar informatiebeveiliging tekortschiet, ligt daar vaak een diepgaandere oorzaak aan ten grondslag die haar oorsprong vindt in een complexe economische dynamiek tussen betrokken actoren aan ten grondslag. Moore en Anderson beschrijven bijvoorbeeld hoe commerciële prikkels producenten ertoe kunnen aanzetten om (nog) gebrekkige hardware en software naar de markt te brengen en hoe het niet hoeven dragen van schade kan leiden tot te weinig aandacht voor beveiliging tijdens de ontwikkeling en het gebruik van ICT producten.[8]

Met juridische maatregelen kan voornoemd gedrag op verschillende manieren worden bijgestuurd.[9] Europese privacy en telecomwetgeving bevat bijvoorbeeld beveiligingsverplichtingen. Telecomwetgeving bevat daarnaast een meldplicht voor incidenten dienaangaande. [10] Deze verplichtingen beogen onder andere (minimum) maatregelen af te dwingen en de verwezenlijking van risico’s inzichtelijk te maken. Er wordt verder gewerkt aan wetgeving die binnen Europa de strafrechtelijke behandeling van aanvallen op ICT-middelen moet harmoniseren. Hiermee wordt beoogd kwaadwillende actoren te ontmoedigen dan wel te straffen.[11] Niet onbelangrijk is verder dat in 2004 het Europees Netwerk en Informatiebeveiliging Agentschap werd opgericht (bekend onder de Engelse afkorting "**ENISA**").[12] ENISA heeft tot taak om de Unie, de lidstaten en (indirect) het bedrijfsleven te helpen om netwerk- en informatiebeveiligingsproblemen het hoofd te bieden. Daartoe onderhoudt zij onder andere een kennisinstituut en helpt zij het gebruik van ICT te professionaliseren. Met name

---

[4] Soms wordt verantwoording (*accountability*) als een apart doel nagestreefd, zodat de onweerlegbaarheid van informatie wordt verzekerd. Opgemerkt moet worden dat het CIA-Model zich primair richt op de beveiliging van informatie. De bescherming van verwerkingsmiddelen wordt niet zelfstandig nagestreefd (bijv. het voorkomen van oneigenlijk gebruik van de apparatuur waarmee informatie verwerkt zoals bij het onttrekken van capaciteit aan systemen zonder informatie aan te tasten).

[5] DG Internal Policies, “*Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*”, IP/A/ITRE/NT/2013-5, September 2013, p. 29 e.v.

[6] Ponemon Istutiute (gesponsored door Symantec), “*2013 Cost of Data Breach Study: Global Analysis*”, mei 2013, p. 7

[7] Volkskrant, “*Telefoonstoring Vodafone houdt hele dag aan*”, 4 april 2012

[8] T. Moore & R. Anderson, “*Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*”, Computer Science Group, Harvard University, 2011

[9] National Research Council “*Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*”, Washington, DC, The National Academic Press, 2010, p. 3 e.v.

[10] Europese Commissie, “*Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union*”, SWD(2013)31, 7 februari 2013, p. 26

[11] Europese Commissie, “*Voorstel voor een richtlijn van het Europees Parliament en de Raad over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad*”, COM(2010)517, 30 september 2010

[12] Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (Pub. L 077 van 13/03/2004 blz. 0001 - 0011)

daartoe zien wij een noodzaak. Het mandaat van ENISA werd tweemaal verlengd, alvorens de positie van ENISA in 2013 werd bestendigd in een nieuwe verordening.[13]

Ondanks bestaande maatregelen en initiatieven op zowel Europees als nationaal niveau constateert de Commissie dat het niveau van beveiliging van netwerk- en informatiesystemen in de Unie over het algemeen onvoldoende is. De Commissie stelt vast dat lidstaten in zeer wisselende mate in staat zijn om problemen het hoofd te bieden, (te) weinig samenwerken en (te) weinig informatie delen. Voor zowel publieke als private actoren geldt dat waar incidenten al opgemerkt worden, deze vaak niet gerapporteerd worden uit angst voor reputatieschade en aansprakelijkheid. Europa is daardoor te kwetsbaar voor elektronische incidenten, risico's en bedreigingen.[14]

Nu veel informatiesystemen onderling met elkaar verbonden zijn en het internet grenzeloos is, hebben beveiligingsrisico's en incidenten veelal grensoverschrijdende oorzaken en gevolgen.[15] Als het vertrouwen in de veiligheid van ICT afbrokkelt dan kan dit het functioneren van de interne markt ondermijnen. De Commissie acht het daarom noodzakelijk om door middel van wetgeving een hoger niveau van beveiliging af te dwingen. Het voorstel voor de NIB-Richtlijn is hiervan het resultaat.[16]

Voorstel voor een richtlijn ter verhoging van de beveiliging van netwerk- en informatiesystemen

De NIB-Richtlijn introduceert maatregelen die een hoog niveau van beveiliging van Informatiesystemen binnen de Europese Unie moeten garanderen. De richtlijn definieert beveiliging als de mogelijkheid van een Informatiesysteem om ongelukken en kwaadwillend handelen te weerstaan dat invloed heeft op het vereiste niveau van beschikbaarheid, authenticiteit, integriteit en confidentialiteit van gegevens of gerelateerde diensten. Risico's zijn omstandigheden of gebeurtenissen die van negatieve invloed kunnen zijn op de beveiliging. Incidenten zijn omstandigheden of gebeurtenissen die een daadwerkelijk negatief effect op de beveiliging hebben.

Interessant is de definitie die de NIB-Richtlijn aan het begrip netwerk- en informatiesysteem ("**Informatiesysteem**") geeft. Dat zijn:

(i) elektronische communicatienetwerken zoals gedefinieerd in Richtlijn 2002/21/EG, namelijk "*de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen die het mogelijk maken signalen over te brengen...*";

(ii) met elkaar verbonden of verwante apparaten die op basis van een programma automatisch gegevens verwerken; en

(iii) digitale gegevens opgeslagen, verwerkt, opgehaald of verzonden worden door middel van de voorgaande voor hun functioneren, gebruik of onderhoud.

Opvallend is dat deze definitie de *data* omvat die worden verwerkt. In de discussies omtrent (de vormgeving van) de NIB-Richtlijn wordt hieraan nauwelijks aandacht besteed. De aandacht gaat veeleer uit naar de technologie waarmee data verwerkt worden. Daarop zijn ook de maatregelen in de richtlijn gericht. Dat op het resultaat van de gebruikte technologie vertrouwd kan worden lijkt ons evenwel juist het eigenlijke doel van de richtlijn. Dat resultaat bestaat uit de geproduceerde data. Zo wil de exploitant van een webwinkel betalingen verwerken en er daartoe van op aankunnen dat de betalingsbevestiging die zij van de bank van haar klant ontvangt juist is. Daartoe moeten de systemen van de bank weliswaar voldoende betrouwbaar zijn, maar die beveiliging is niet het enige noch het eigenlijke doel. De vraag is of deze nuance in het voorstel voor de NIB-Richtlijn voldoende onderkend wordt. Het risico bestaat anders dat het initiatief ondoelmatig is.

---

[13] Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad van 21 mei 2013 inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004 (Pub. L 165 van 18/06/2013 blz. 0041 - 0058)

[14] Idem., zie: COM2013(48), p. 3

[15] Een systeem in Nederland kan bijvoorbeeld door een hacker in Italië worden aangevallen. Andersom vertrouwden partijen over de hele wereld ten onrechte op de integriteit van digitale certificaten die door Diginotar in Nederland werden beheerd. Toen haar systemen gecompromitteerd bleken te zijn, was het voor de aanvaller mogelijk om zich online als anderen voor te doen. Dit leidde er bijvoorbeeld toe dat dat de e-mail van Iraanse dissidenten op Google servers kon worden afgeluisterd. Zie: The Guardian, "*Diginotar SSL certificate hack amounts to cyberwar, says expert*" 5 september 2011

[16] Idem., zie: COM2013(48), p. 3

Beschouwen wij de wijze waarop de NIB-Richtlijn haar doelstelling beoogt te verwezenlijken dan stellen wij vast dat zij daartoe drie categorieën van maatregelen introduceert, namelijk:

(i) vereisten waaraan lidstaten moeten voldoen om de beveiliging van Informatiesystemen te garanderen en om daarnaast om te kunnen omgaan met risico's en incidenten;

(ii) verplichtingen voor lidstaten om gecoördineerd uitvoering te geven aan de vereisten van de NIB-Richtlijn; en

(iii) beveiligingsvereisten voor aangewezen categorieën van publieke en private partijen.

We gaan hierop hierna nader in. Op voorhand stellen wij vast dat de NIB-Richtlijn zelf geen methodologie aanwijst of criteria formuleert om aan een gewenst of vereist niveau van beveiliging uitdrukking te geven. De vraag is hoe de ambities van de NIB-Richtlijn geobjectiveerd zouden kunnen worden om haar effectiviteit (beter) te kunnen beoordelen. Ten aanzien van informatiebeveiliging in brede zin en beschikbaarheid (*availability*) in het bijzonder kan gedacht worden aan bereikbaarheid gedurende een periode (bijv. in de zin van service level afspraken). Objectieve criteria voor confidentialiteit, integriteit en verantwoording laten zich lastiger formuleren. Het gevolg daarvan is dat in de praktijk een toevlucht gezocht wordt tot het specificeren van maatregelen of *controls* die bepaalde doeleinden of *control objectives* dienen.[17] Toetsing daarvan (zoals bijvoorbeeld in audits) is administratief inspannend en biedt desondanks weinig zekerheid omtrent de mate van beveiliging.

Vereisten voor de afzonderlijke lidstaten

Een vereiste om binnen de Unie een hoger algemeen niveau van beveiliging van Informatiesystemen te bewerkstelligen, is dat alle lidstaten beschikken over vergelijkbare (minimale) capaciteiten om dreigingen, risico's en incidenten het hoofd te bieden. Dat is nu niet het geval en de NIB-Richtlijn beoogt daarin verandering te brengen door lidstaten te verplichten om tenminste bepaalde activiteiten te ondernemen en om daartoe de nodige organisatorische structuren voor in het leven te roepen.

Bewerkstelliging van een hoog beveiligingsniveau

De richtlijn legt lidstaten een verplichting op om binnen hun grondgebied zorg te dragen voor een hoog niveau van beveiliging van Informatiesystemen (artikel 4). Anders dan dat hiermee een ambitie wordt uitgesproken, is de vraag wat vervolgens moet kwalificeren als een (voldoende) hoog niveau van beveiliging. In navolging van ons algemene commentaar op het voorstel vragen wij ons bij gebreke van objectieve criteria af of het exacte doel van de NIB-Richtlijn voldoende nauwkeurig bepaald is en of de te stellen normen daaraan voldoende dienstbaar zijn. Het voorstel werkt nu in haar algemeenheid (minimum) activiteiten uit die lidstaten moeten ondernemen (waarover hierna meer). Zonder dat expliciet tot doel te stellen lijken deze activiteiten sterk gericht op het verhogen van de weerbaarheid tegen kwaadwillend handelen en te weinig op het bestrijden van de problematiek in meer fundamenteel opzicht.

Onderhoud van een cybersecurity strategie

De NIB-Richtlijn vereist dat iedere lidstaat tenminste een nationale netwerk- en informatiebeveiligingsstrategie onderhoudt. Dit dient strategische doelstellingen ter verhoging van de beveiliging van netwerk- en informatiesystemen te identificeren, alsmede het beleid en de maatregelen die ter verwezenlijking daarvan zullen worden genomen (artikel 5).

Het voorstel specificeert een vijftal punten waaraan een beveiligingsstrategie tenminste moet voldoen. In de eerste plaats moeten doelstellingen en prioriteiten worden bepaald naar aanleiding van een actuele analyse van risico's en incidenten en er moet een bestuursmodel worden ingericht om deze doelstellingen te realiseren. De strategie moet verder in algemene zin mogelijke (voorbereidings-, reactie- en herstel-)maatregelen beschrijven die bij incidenten getroffen moeten worden en lijnen uitzetten voor opleidingsprogramma's, bewustwordingscampagnes en programma's voor speur- en ontwikkelwerk. De nationale strategie moet een apart samenwerkingsplan bevatten waarin taken, verantwoordelijkheden en procedures van de betrokken actoren worden vastgelegd. Een onderdeel hiervan is bijvoorbeeld het plan aan de hand waarvan risico's beoordeeld moeten worden.

[17] Zoals bijvoorbeeld uitgewerkt in de ISO/IEC 27000 standaarden.

Zowel verschillende Europese lidstaten als landen buiten de Europese Unie onderhouden al enige tijd eigen cyber security strategieën.[18] Nederland doet dat sinds 2011 en publiceerde onlangs de opvolger van haar eerste strategie.[19] Een belangrijk onderdeel van de Nederlandse strategie is het Cyber Security Beeld Nederland.[20] De focus daarvan ligt wellicht nog (te) beperkt op kwaadwillende actoren en het reageren daarop en dit vormt nog in sterke mate het beleid. Desalniettemin onderhoudt Nederland hiermee ons inziens het meest fundamentele en straks vereiste onderdeel om een succesvol beleid op te kunnen baseren. Het huidige beleid incorporeert ook veel van de vereisten die de NIB-Richtlijn beoogt te stellen. Op het terrein van governance en samenwerking moeten taken, rollen en verantwoordelijkheden verder uitkristalliseren, maar dat wordt onderkend. Op het terrein van onderwijs zal een publiek-private taskforce Cybersecurity Onderwijs worden ingericht.[21] Er wordt al een onderzoeksagenda onderhouden.[22] Hoewel er ruimte is voor verbetering, ligt hiermee een fundament waar de vereisten uit de NIB-Richtlijn ons inziens nauwelijks aan toevoegen.

Aanwijzing van een nationale competente autoriteit

De NIS-richtlijn vereist dat lidstaten een nationale autoriteit aanwijzen – en met voldoende middelen toerusten – om toe te zien op de naleving van de verplichtingen daaruit. De lidstaten moeten er bovendien op toezien dat deze autoriteit middels het samenwerkingsverband dat de richtlijn daartoe schept (zie hierna) adequaat samenwerkt met de autoriteiten uit de andere lidstaten (artikel 6).

De vraag of er een (centrale) autoriteit moet komen voor de beveiliging van Informatiesystemen is van fundamentele aard. De keuze voor een centrale autoriteit lijkt voor de hand te liggen als informatiebeveiligingsproblemen als een generiek en zelfstandig ICT probleem gezien worden. Centralisering faciliteert dan een eenduidige aanpak, mede in internationaal verband. De vraag is evenwel of sprake is van een generiek en zelfstandig ICT probleem.

Informatiesystemen zijn dienend aan bedrijfsprocessen. Informatiebeveiliging lijkt een aspect van een kwalitatief hoogwaardige informatieverwerking binnen het gediende proces en lijkt daarvan moeilijk los gezien te kunnen worden. Als dit zo is, behoort de instantie die verantwoordelijk is voor toezicht op het bedrijfsproces anno 2014 dan niet over de capaciteit te beschikken om toe te kunnen zien op de veiligheid van gebruikte systemen? Ook als sprake is van een zelfstandig probleem, moet bedacht worden dat beveiligingsproblemen hun oorsprong zowel in de techniek als in het gebruik daarvan vinden. Beiden kunnen bijvoorbeeld sterk verschillen per sector. Hetzelfde geldt voor de potentiële gevolgen van incidenten. Het zal bijvoorbeeld uitmaken of een systeem betalingsverkeer ondersteunt, de luchtverkeersleiding assisteert of een drinkwaterzuiveringssysteem bedient. Dit alles maakt dat per sector een andere, meer of minder vergaande aanpak nodig kan zijn.

Op basis van het voorgaande lijkt verantwoordelijkheid voor de veiligheid van Informatiesystemen thuis te horen bij de instantie die verantwoordelijk is voor het toezicht op de met die systemen gediende processen. Dat hoeft Europese samenwerking niet te belemmeren. Sterker nog, veel sectorale toezichthouders werken al samen in Europees verband. Het bestaan van geoliede samenwerkingsverbanden kan de invoering van nieuwe wetgeving aanzienlijk versnellen. Gezien de urgentie van de problematiek zou dat geen overbodige luxe zijn. Wij vragen ons daarom af de NIB-Richtlijn er goed aan doet om het inrichten van nieuwe centrale nationale autoriteiten dwingend voor te schrijven. Zo de keuze voor een centrale autoriteit al gemaakt kan worden, lijkt ons dat lidstaten zelf het beste in staat zijn om dit te beoordelen.

De NIB-Richtlijn erkent overigens dat de aangewezen toezichthouder bij het uitvoeren van haar taken in het vaarwater van andere instanties zal komen. Zij wordt daarom verplicht om *incidenten* die vermoedelijk samenhangen met (zware) criminele activiteiten te melden bij justitiële autoriteiten. Bij het behandelen van incidenten waarbij persoonsgegevens betrokken zijn, dient zij samen te werken met de autoriteiten op het gebied van de privacybescherming. Overlap met vereisten uit andere rechtsgebieden

[18] ENISA, "*National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace*", 8 mei 2012. ENISA houdt op haar website een actueel overzicht bij van de stand van zaken. Zie http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss.
[19] Ministerie van Veiligheid en Justitie, "*Nationale Cyber Security Strategie 2 (NCSS 2) - Van bewust naar bekwaam*", 28 oktober 2013
[20] Ministerie van Veiligheid en Justitie (NCSC), "*Cybersecuritybeeld Nederland CSBN-3*", juni 2013
[21] Idem., zie: NCSS 2, p. 19
[22] ICT Innovatie Platform Veilig Verbonden, "*National Cyber Security Research Agenda II*", 30 september 2013

ligt voor de hand en het risico bestaat dat dubbele of zelfs conflicterende vereisten in het leven geroepen worden. Er kunnen ook lacunes ontstaan. Dit alles heeft veel invloed op de kosten voor naleving van de regelgeving en kan de effectiviteit daarvan sterk ondergraven. Dit vraagt daarom specifieke aandacht tijdens het wetgevingsproces.

Overigens wordt een van de specifieke taken van de aangewezen nationale autoriteit om toezicht te houden op de naleving van de beveiligingsplicht en de meldplicht voor incidenten die de NIB-Richtlijn oplegt. Daartoe wordt haar de mogelijkheid gegeven om partijen te onderwerpen aan beveiligingsaudits door gekwalificeerd onafhankelijke lichamen of autoriteiten. Onduidelijk is op welk soort onafhankelijk lichaam of autoriteiten het voorstel doelt; vallen daaronder ook commerciële auditors? Wordt hiermee niet impliciet een mogelijkheid geschapen om de beoogde partijen tot certificering te dwingen? Ruimhartig gebruik van een dergelijke bevoegdheid kan verschillen in het leven roepen tussen lidstaten. Dit risico vraagt om nadere aandacht.

Inrichting van een nationaal Computer Emergency Response Team

In aanvulling op het aanstellen van een autoriteit voor de beveiliging van Informatiesystemen, vereist de NIB-Richtlijn dat iedere lidstaat een zogenaamd Computer Emergency Response Team ("**CERT**") inricht (artikel 7). Dat is een organisatie die beveiligingsincidenten helpt voorkomen en helpt ingrijpen wanneer deze zich voordoen. ENISA stelt dat "*like a fire brigade, they are the only ones which can react when security incidents occur*".[23] Het op te richten CERT moet handelen onder toezicht van de op grond van de richtlijn aangewezen nationale beveiligingsautoriteit. Het mag daarvan ook een onderdeel zijn. Nederland heeft reeds zo'n nationaal CERT als onderdeel van het Nationale Cyber Security Centrum dat opereert als onderdeel van het Ministerie van Veiligheid en Justitie.

Wij onderschrijven het belang van het hebben van een CERT, maar wijzen ook op de beperkingen van haar rol bij het adresseren van de algehele problematiek waar de NIB-Richtlijn zich op richt. Die wordt overschat door het soms levende idee dat het voornaamste dat we nodig hebben een team "computerhelden" is of, om aan te haken op gebruikte analogieën, een digitale brandweer. Gegeven de eerder beschreven fundamentele oorzaken van beveiligingsproblemen behoren zij in de eerste plaats te worden aangepakt in de bedrijfsprocessen waartoe zij behoren en de ICT beheerorganisaties die daaraan dienstbaar zijn. Daar ligt de verantwoordelijkheid voor de dagelijkse gang van zaken en bestaat het overzicht om fundamentele bescherming tegen incidenten vorm te kunnen geven (incl. het inplannen van back-up voorzieningen en het onderhouden van beveiligingsbeleid en disaster-recovery plannen). Slechts bepaalde incidenten horen bij een CERT thuis. Men denke inderdaad aan incidenten door toedoen van kwaadwillend handelen. Het voorstel erkent dit onderscheid onvoldoende.

Verplichte samenwerking tussen de lidstaten

Vanwege het reeds gememoreerde mondiale karakter van het internet kunnen risico's en incidenten grensoverschrijdende oorzaken en gevolgen hebben. De Commissie is van mening dat het daarom noodzakelijk is om lidstaten te verplichten tot samenwerking bij het bestrijden hiervan.[24]

Een geïnstitutionaliseerd samenwerkingsverband

De aangewezen autoriteiten in de lidstaten en de Commissie moeten een samenwerkingsverband vormen waarbinnen zij continue met elkaar in verbinding staan en structureel met elkaar samenwerken bij het bestrijden van risico's en incidenten (artikel 8). Noemenswaardig is dat de NIB-Richtlijn voor de Unie ook de mogelijkheid schept om overeenkomsten aan te gaan met niet-lidstaten voor deelname aan de activiteiten van het samenwerkingsverband (artikel 13). Vanuit het Parlement is bovendien geopperd om ook de mogelijkheid te formaliseren dat private partijen deelnemen aan bijvoorbeeld het uitwisselen van kennis, capaciteitsopbouw en oefeningen.[25]

Het verband dient samen te werken rondom het onderhouden van nationale NIS strategieën en daarmee gemoeide capaciteiten (bijvoorbeeld door coördineren van kennisoverdracht en het

[23] ENISA, "*Factsheet: Emergency Response to Security Breaches*", 14 mei 2009
[24] Idem, zie: SWD(2013)31, 7 februari 2013, p. 32
[25] Zie Amendement 41 en toelichting op pagina 53, European Parliament (Committee on the Internal Market and Consumer Protection), Draft Report, 2013/0027(COD), 10 juli 2013, Amendment 41 en p. 53 and Europees Parlement (Committee on Industry, Research and Energy), Draft Opinion, 2013/0027(COD), 19 november 2013, amendement 263

ondernemen van oefeningen). Van belang is dat de NIB-Richtlijn de bevoegde autoriteiten van lidstaten ertoe verplicht om elkaar te waarschuwen voor bepaalde gekwalificeerde risico's en incidenten. Dit is het geval wanneer deze snel in omvang toenemen, nationale reactiecapaciteit te boven gaan of meer dan een lidstaat treffen dan wel daartoe de potentie hebben (artikel 10). De autoriteiten moeten hun reacties op dergelijke grensoverschrijdende incidenten via het samenwerkingsverband coördineren (artikel 11).

De Commissie krijgt vergaande bevoegdheden om de samenwerking van het verband vorm te geven. Zij kan op eigen initiatief door middel van uitvoerende handelingen maatregelen nemen om activiteiten van het samenwerkingsnetwerk te ondersteunen. Het comité dat de NIB-Richtlijn in het leven roept om de Commissie bij te staan heeft hierbij slechts een adviserende rol (artikel 8 lid 4). De Commissie krijgt daarnaast de bevoegdheid om middels (door het comité toetsbare) uitvoeringshandelingen een samenwerkingsplan voor de Unie te onderhouden. De bedoeling is dat zij hierin de procedures uitwerkt volgens welke de samenwerking tussen lidstaten moet verlopen bij het uitwisselen van waarschuwingen en het coördineren van acties, alsmede de NIB-capaciteitsopbouw coördineert door het opstellen van programma's voor opleiding en kennisoverdracht en gezamenlijke oefeningen (artikel 12). De vraag is of deze bevoegdheden niet te vergaand ingrijpen in de nationale aanpak van beveiligingsproblemen door lidstaten. Bedenk dat de problematiek door veel lidstaten niet louter als een aspect van handelspolitiek gezien wordt, maar ook van nationale veiligheid en defensie. Ons inziens wordt vanuit het Parlement terecht voorgesteld om het samenwerkingsplan te veralgemeniseren tot een raamwerk, verplichtingen minder dwingend te maken en deze bovendien door middel van gedelegeerde wetgeving vorm te laten geven.[26]

Beschikbaarheid van een veilige infrastructuur

Om de beoogde samenwerking tot stand te kunnen brengen moeten lidstaten informatie kunnen delen. Met name bij het samen het bestrijden van risico's en incidenten kan dat ook zeer gevoelige informatie betreffen, zoals bijvoorbeeld kwetsbaarheden in betrokken systemen.[27] Los van de activiteiten die het samenwerkingsverband van lidstaten moet ontplooien, stelt de NIB-Richtlijn daarom eisen aan het middel waarmee informatie kan worden uitgewisseld.

Voor de uitwisseling van gevoelige informatie moeten de lidstaten gebruik maken van een veilige gemeenschappelijke infrastructuur (artikel 9). Lidstaten moeten aan voorwaarden voldoen om hierop aangesloten te mogen worden en om zo toegang te kunnen krijgen tot vertrouwelijke informatie uit andere lidstaten.[28] Deze voorwaarden kunnen betrekking hebben op (i) de beschikbaarheid van een veilig, betrouwbaar en compatibel nationaal communicatiemedium en (ii) de toereikendheid van de middelen om aan het beveiligde netwerk te kunnen deelnemen. De bevoegdheid om deze criteria nader in te vullen wordt gedelegeerd aan de Commissie. Die beslist vervolgens (in de vorm van een uitvoeringshandeling) per geval over het verlenen van toegang aan de lidstaten.

De preambule van de NIB-Richtlijn legt een nadruk op dit beveiligde samenwerkingsmechanisme die de eigenlijke activiteiten die het samenwerkingsverband zal ontplooien lijkt te overschaduwen.[29] Als wij ENISA goed begrijpen, is de voornaamste uitdaging in Europees verband het gebrek aan een algemeen geaccepteerd (veilige) communicatiemiddel.[30] De gekozen insteek komt ons daartoe erg zwaar over. Zo de richtlijn een specifiek communicatiemiddel zou moeten voorschrijven, kan dan niet volstaan worden met een aan de Commissie opgedragen uitvoeringshandeling?

Verplichtingen voor publieke en (geselecteerde) private partijen

Veel Informatiesystemen die voor het functioneren van de samenleving van vitaal belang zijn, worden beheerd door private partijen. Dat is (indirect) vaak ook het geval waar het overheidssystemen betreft, omdat die ook vaak afhankelijk zijn van diensten die worden aangeboden door systemen in beheer van

[26] Zie Amendementen 282-284, Europees Parlement (Committee Industrie, Onderzoek en Energie), Concept Opinie, 2013/0027(COD), 19 november 2013
[27] ENISA, "*Proactive detection of network security incidents*", 7 december 2011. Zie voor een nadere beschouwing daarvan ook P. Kijewski en P. Pawliński (CERT Polska), "*Proactive Detection and Automated Exchange of Network Security Incidents*", STO-MP-IST-111
[28] Idem., zie: COM(2013)48, overweging (12) en (14), p. 14
[29] Idem., zie: COM(2013)48, overweging (12) en (14), p. 14
[30] ENISA, "*Secure Communication with the CERTs & other stakeholders*", 21 december 2011

private partijen. Een beleid dat gericht is op het verhogen van het algehele niveau van netwerk- en informatiesysteembeveiliging in de Unie moet zich daarom ook tot private partijen uitstrekken.[31] De NIB-Richtlijn richt zich daarom apart tot overheidsinstanties en (geselecteerde) private partijen (artikel 14).

Kern: het treffen van beveiligingsmaatregelen en het melden van incidenten

De NIB-Richtlijn verplicht aangewezen partijen ertoe om passende (technische en organisatorische) maatregelen te nemen ter controle van de risico's die de Informatiesystemen die zij controleren en gebruiken bij hun activiteiten lopen. Die maatregelen moeten in de eerste de impact van incidenten op kerndiensten van deze partijen beperken. Zo moet de continuïteit van deze diensten gegarandeerd worden. Het gehanteerde niveau van beveiliging moet passend zijn gezien de risico's die gelopen worden (artikel 14).

De NIB-Richtlijn beoogt bij de uitvoering van de beveiligingsplicht het gebruik van algemene normen en specificaties voor beveiliging te stimuleren (artikel 16). De Commissie krijgt daartoe in het voorstel de bevoegdheid om bij uitvoerende handeling een lijst met standaarden te onderhouden. De NIB-Richtlijn bepaalt niet welke status deze lijst heeft en hoe vrijblijvend het gebruik van genoemde standaarden moet zijn. Moet de toepassing daarvan bijvoorbeeld leiden tot erkenning van een adequate beveiliging? Afhankelijk hiervan krijgt de Commissie verregaande invloed in de acceptatie van standaarden, hetgeen een sterk verstorend effect op de markt kan hebben. Ten onrechte opgenomen standaarden zouden mogelijk als norm geïmplementeerd en wellicht zelfs gehandhaafd worden en niet genoemde maar meer geschikte standaarden zouden ten onrechte door de markt genegeerd kunnen worden. De vraag is of dit dienstbaar is aan het doel van de NIB-Richtlijn.

Incidenten worden door getroffen partijen vaak zoveel mogelijk geheim gehouden uit vrees voor reputatieschade en aansprakelijkheden.[32] Naast een verplichting om Informatiesystemen te beveiligen, wordt daarom ook een wettelijke plicht ingesteld om incidenten te melden wanneer die een significante invloed hebben op de beveiliging van de kerndiensten van de daaraan onderworpen partijen (artikel 14 lid 2). De toezichthouder kan vervolgens in het algemeen belang besluiten een incident publiekelijk bekend te maken of de meldende partij verplichten dat te doen (artikel 14 lid 2).

Vanuit de toepassing gedacht is belangrijkste vraag wellicht of de definitie van een incident voldoende duidelijk is. Wat kwalificeert er voorts als een incident met significante invloed en wat exact behoort er tot de kerndiensten van een partij? Wat moet er vervolgens gemeld worden? Illustratief voor de inhoud van een melding is wellicht de meldplicht die inmiddels geldt voor aanbieders van openbare elektronische communicatiediensten.[33] Die meldplicht ziet evenwel op incidenten die betrekking hebben op persoonsgegevens. Dat brengt ons op een ander punt.

De richtlijn introduceert een zoveelste meldplicht voor (beveiligings)incidenten.[34] Een fundamenteel punt is dat het laatste waar een partij tijdens een incident aandacht aan zal kunnen (en zou moeten) besteden de coördinatie van de relaties met verschillende toezichthouders tegelijk is. Overlappende verplichtingen en toezicht maken compliance namelijk bijzonder complex. Die complexiteit maakt het bovendien erg belastend. De kostenramingen van de Commissie lijken onrealistisch laag.[35] Men realiseren zich dat incidenten met een zekere omvang moeten gemeld moeten worden. De opvolging van grotere incidenten is een multidisciplinaire aangelegenheid waarbij naast de IT afdeling verschillende afdelingen binnen een onderneming betrokken zijn. Gebruikelijk is bijvoorbeeld dat onafhankelijke forensische experts assisteren bij het boven water krijgen van de juiste informatie. Meldingen en publicaties worden verder doorgaans in samenwerking met de juridische afdeling of communicatieafdeling opgesteld. Een deel van deze activiteiten zou zonder de voorgestelde meldplicht ook nodig zijn, maar een melding aan een toezichthouder vraagt evengoed om specifieke aandacht. Dat is temeer het geval wanneer het nalaten van een melding of het indienen van een onjuiste melding gesanctioneerd kan worden. De opvolging van een melding door een toezichthouder zal de noodzakelijke inspanning alleen verder vergroten. Dit alles leidt tot aanzienlijke extra kosten. Het lijkt ons raadzaam om meer aansluiting te zoeken bij bestaande meldplichten en meldingen waar mogelijk bij een enkele instantie te laten doen.

---

[31] Idem., zie: SWD(2013)31, p. 15
[32] Idem., zie: SWD(2013)31, p. 15
[33] Artikel 4 Richtlijn 2009/136/EC, uitgewerkt in Verordening 611/2013
[34] Mr. ir. J.M. van Essen, "*Nieuwe meldplichten in privacyland*", P&I 2013/5, p. 218
[35] Idem., zie: SWD(2013)31, p. 91 e.v.

Indien gevoelige gegevens (zoals kwetsbaarheden of persoonsgegevens) gemeld moeten worden is de vraag hoe of dit geoorloofd is en hoe die beschermd moeten worden tegen oneigenlijk gebruik.[36] De Rabobank merkte recentelijk bijvoorbeeld op dat haar meldingen in beginsel onder de openbaarheid van bestuur vallen. Zij achtte dat problematisch, omdat meldingen de configuraties en kwetsbaarheden van Informatiesystemen van zowel haarzelf als andere partijen kunnen prijsgeven. De Rabobank pleitte er op die grond voor om meldingen aan te merken als staatsgeheim.[37] Nu lijkt dit ons het noodzakelijke verder kunnen delen van informatie voorbij te schieten, maar de zorg van Rabobank is daarom niet minder begrijpelijk en de vraag is hoe daarmee om moet worden gegaan.

Wij menen dat verduidelijking op voorgaande punten gediend zou zijn met een discussie omtrent het doel van de meldplicht.[38] Daarvoor lijkt vooralsnog weinig aandacht. Dit is wel vereist om een belastende maatregel als deze te kunnen legitimeren. Helderheid omtrent het doel is nodig om de voor een melding benodigde informatie te bepalen. Al naar gelang het gediende doel kunnen ook andere details van de meldplicht vormgegeven worden: wat is een meldingsplichtig incident, aan wie moet er gemeld worden, wat gaat die partij met een stortvloed aan meldingen doen en wat gaat het kosten om daar iets zinvols mee te doen? De rechtszekerheid is er niet mee gediend als de Commissie dit achteraf kan bepalen op grond van gedelegeerde wetgeving en uitvoeringshandelingen (artikel 14 leden 5 en 7). Alleen een zuivere afbakening maakt het mogelijk een effectieve regeling op te stellen.

Daargelaten het doel die een eventuele meldplicht moet dienen, moet de vraag gesteld te worden of er geen geschiktere alternatieven zijn. Denkbaar is dat een vrijwaring voor aansprakelijkheden (zoals die onder omstandigheden in de VS bestaat) ook voldoende overzicht en inzicht biedt ten aanzien van incidenten. Het invoeren van een verzekeringsplicht tegen schade ten gevolge van cyber incidenten zou de handhaving van een adequaat beveiligingsniveau door wellicht kunnen verplaatsen naar de markt. Er zijn legio andere mogelijkheden denkbaar. Die zouden wij gezien de hiervoor geplaatste kanttekeningen nader overwegen alvorens een meldplicht in te voeren.

Verdere keuzes omtrent de implementatie

De richtlijn richt zich tot geselecteerde categorieën private spelers. Daaronder vallen (i) aanbieders van diensten van de informatiemaatschappij die de levering van dergelijke diensten door anderen mogelijk maken en (ii) beheerders van infrastructuur die van vitaal belang is voor economische en maatschappelijke functies voor energielevering, transport, bancaire dienstverlening, aandelenbeurzen en gezondheidszorg. De richtlijn bevat een indicatieve lijst van partijen in beide categorieën. Zorgelijk is wellicht de uitwerking van de eerste categorie met daarin "*e-commerce platforms*" en "*cloud computing services*", hetgeen ertoe leidt dat praktisch alle partijen die diensten via internet ontsluiten binnen bereik komen. De vraag is of het doel van de richtlijn dat rechtvaardigt. ECOSOC stelt het andere uiterste voor en wil lidstaten verplichten onderworpen partijen aan te wijzen en in een publiek register op te nemen.[39] Een gepaste tussenoplossing zou mogelijk moeten zijn.

De richtlijn zondert micro ondernemingen vervolgens uit van haar werkingssfeer. De vraag is of dit terecht is. Informatietechnologie stelt juist (relatief) kleine ondernemingen in staat om cruciale diensten aan te bieden, waarbij gemakkelijk grote hoeveelheden gevoelige gegevens verwerkt worden. Nu de verplichtingen risico-gestuurd moeten zijn, zou het niet onverstandig zijn deze partijen binnen bereik van de richtlijn te houden. Met hun positie kan wellicht beter rekening gehouden worden bij de handhaving. Terecht adviseert ECOSOC voorts om aandacht te besteden aan de kennis en vaardigheden van kleine spelers - kennis die anders juist voor hen ontoegankelijk is.[40]

---

[36] ENISA, "*A flair for sharing – encouraging information exchange between CERTs*", 16 december 2011
[37] Financieel Dagblad, "*Onvrede over aanpak cybercrime*", 29/10/2013
[38] Een meldplicht kan verschillende doelen dienen. Het kan inzicht geven in (de kans op verwezenlijking van) risico's, hetgeen in de eerste plaats technische informatie over het incident vereist. In economische termen maakt dit het beprijzen van risico's mogelijk. Dit stelt partijen in staat om op rationele gronden tegenmaatregelen te nemen. Technische informatie zou ook nodig zijn als de gemelde informatie er toe moet dienen om de adequaatheid van de getroffen maatregelen te controleren. Daartoe is technische informatie over die maatregelen nodig (incl. een beschrijving van de maatregelen die gefaald hebben of ontbraken). Een meldplicht kan er verder toe dienen om derden tijdig schadebeperkende maatregelen te laten treffen. Dit vraagt eerder om inzicht in aspecten van tijdstip en causaliteit dan om diepgaande technische informatie.
[39] Zie overweging 1.13, ECOSOC EG, "Opinion of the European Economic and Social Comittee - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union - COM(2013)48 final - 2013/0027(COD)", 22 mei 2013
[40] Idem., zie: ECOSOC EG, Overweging 1.10 en 3.5

Interessant is voorts dat de richtlijn slechts gebruikers van informatietechnologie adresseert. Veel incidenten vinden evenwel juist hun oorsprong in de producten die gebruikt worden.[41] Die zijn in veel gevallen het gevolg van het onprofessioneel *ontwikkelen* daarvan, al dan niet versterkt door perverse prikkels om producten zo snel mogelijk naar de markt te krijgen.[42] Dit onderkent ook ECOSOC, dat aanbeveelt om mogelijkheden te scheppen voor verhaal van schade op producenten in zoverre gebreken in hun producten bijdragen aan incidenten.[43] Hoewel dat tot praktische problemen van geheel eigen aard zal leiden (causaliteit is veelal moeilijk vast te stellen), sluiten wij ons aan bij het principe dat producenten bij het adresseren van deze problematiek betrokken moeten worden.

Conclusie

De Commissie acht het niveau van beveiliging van Informatiesystemen in de Unie onvoldoende en acht dit een risico voor het functioneren van de interne markt. Zij heeft een strategie geformuleerd om het niveau van beveiliging te verhogen. Het voorstel voor de NIB-Richtlijn van begin 2013 is een van de concrete acties ter uitvoering daarvan.

In zowel de Raad als het Europees Parlement is het voorstel in beginsel positief ontvangen. In de Raad is daarover in 2013 meerdere keren overlegd. Naar wij begrijpen vindt evenwel nog steeds hevige discussie plaats over fundamentele aspecten daarvan en is nog geen nader standpunt ingenomen over de verder gewenste vormgeving. Vanuit het Europees Parlement zien wij concretere initiatieven, waaronder gedetailleerde amendementen. Van het Parlement wordt verwacht dat zij eind januari 2014 haar definitieve positie bekend zal maken.

Wij onderkennen dat de beveiliging van Informatiesystemen aandacht behoeft en wij onderschrijven de noodzaak van Europees gecoördineerd handelen. Wij vragen ons af of de NIB-Richtlijn hieraan in haar huidige vorm optimaal bijdraagt. De huidige stand van het initiatief biedt ruimte om onbenutte kansen alsnog te gebruiken en om praktische bezwaren nader te overwegen. Wij beperken ons tot onze belangrijkste observaties.

Een fundamenteel punt van kritiek is dat de discussies rondom de vormgeving van de NIB-Richtlijn teveel uitgaan van het bestrijden van incidenten door toedoen van kwaadwillend handelen. Als de invulling van de te introduceren verplichtingen (zoals het onderhouden van cyber security strategieën en gestructureerde samenwerking) die lijn volgt, wordt de eigenlijke problematiek miskend en zullen maatregelen beperkt effect sorteren. De doelstellingen van de NIB-Richtlijn zouden daarom nader en nadrukkelijker moeten worden overwogen en afgebakend.

Het voorstel erkent dat het belangrijk is om de private sector te adresseren en schept daartoe onder andere voor hen een beveiligingsverplichting en een meldplicht voor incidenten. De invoering van deze verplichtingen en de gekozen vorm daarvoor pakken mede daarom onvoldoende effectief uit. In het licht daarvan legitimeert de Commissie de noodzaak daartoe onvoldoende. Er moet duidelijker bepaald worden welke doeleinden de verplichtingen dienen. Nu worden zij aan dermate brede categorieën van partijen opgelegd dat de beoogde proportionaliteit ontbreekt: met de opname van e-commerce en cloud aanbieders komen in feite alle aanbieders van moderne software en online diensten binnen de toepassingssfeer. Tegelijkertijd worden producenten van ICT producten en micro-ondernemingen uitgezonderd, terwijl zij juist veel risico's veroorzaken. De meldplicht is verder weinig concreet in wat zij van onderworpen partijen vraagt en zal in haar huidige vorm onnodig belastend zijn. Een ander punt is dat de beveiligingsnorm in haar huidige vorm een risico herbergt om de markt te verstoren door de Commissie technische standaarden te laten aanwijzen.

Informatiebeveiliging wordt in de discussie rondom het voorstel teveel als een zelfstandig probleem gezien. Illustratief is ook de wens om hiervoor een aparte richtlijn op te stellen, om iedere lidstaat te verplichten om een centrale autoriteit aan te wijzen voor toezicht daarop en om af te dwingen dat iedere lidstaat een CERT in het leven roept. Wij benadrukten al dat informatiebeveiliging een eigenschap is van een kwalitatief hoogwaardige informatiehuishouding. Meer dan aandacht voor beveiliging en nieuwe beveiligingsmechanismen en producten is aandacht vereist voor hoogwaardige(re) technologie en professioneel gebruik daarvan. Voor het stimuleren daarvan kan onder andere gedacht worden aan het

[41] Idem., zie: Ponemon, p. 7
[42] T. Moore & R. Anderson, "*Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*", TR-03-11, Computer Science Group, Harvard University, 2011
[43] Idem., zie: ECOSOC EG, Overweging 1.10 en 4.9

introduceren van financiële (bijv. subsidies) en juridische prikkels (bijv. aansprakelijkheden). Het zou de Commissie sieren om een fundamentelere aanpak niet te schuwen.